Technical Information

レコーダ&データロガー / 小規模計装機器向け セキュリティ対策基準

TI 04A02A01-00JA

目　次

1. はじめに

横河電機株式会社およびグループ会社におけるセキュリティへの取り組み

YOKOGAWAは、お客様資産に対するサイバー攻撃の脅威について、お客様が安心、安全に事業活動を継続できるよう、お客様と共に取り組む事を理念とし、製品の開発から始まり、システム導入時のセキュリティ対策の実装、運用時のセキュリティ管理まで、お客様のセキュリティ活動をライフサイクルにわたりサポートしています。
製品開発の段階では、ソフトウェアの内部構造や導入する技術に起因する脆弱性を排除するように努め、出荷後に発見された脆弱性や新たに発生した脅威については、適切に対応できるよう体制を整えています。
このようなサイバー脅威への取り組みの一つとして、製品への脆弱性の作りこみや混入を防止すべく、Yokogawa PSIRT (Product Security Incident Response Team)を中心に継続的な脆弱性ハンドリングを行っています。
YOKOGAWA製品の脆弱性にお気づきの際は、psirt@ml.jp.yokogawa.comまでご連絡ください。

さらに、YOKOGAWAでは、ステークホルダーの皆様から信頼をいただいてお預かりする大切な情報を守るため、ISO27001の考え方に基づいて、ITの観点から情報セキュリティ対策に取り組んでいます。

このドキュメントは、横河電機のネットワークソリューション事業部が提供する製品に対するセキュリティ対策のガイドラインです。このドキュメントでは、対象製品のネットワーク（Ethernet）接続におけるリスクアセスメントおよびセキュリティ対策について一般化し、標準的なモデルに基づいて管理する方法について説明します。
本ドキュメントは、日々進化するセキュリティ上の脅威に対抗するために、予告なく更新されることがあります。

セキュリティの必要性

近年、ネットワーク、情報技術の発展により制御システムにおいても、オペレーティングシステム（OS）や通信プロトコルなどを中心に情報システムで採用されているオープンな技術が取り入れられています。このことが、情報システムと制御システムの緊密な連携を加速しています。

一方このような環境では、制御システムが、悪意を持った攻撃者の標的にされ、コンピュータウィルスに代表される不正なプログラムによってセキュリティ上の脅威にさらされることになります。計測システム、あるいは制御システムを安全な状態に保つことは、資産を保護する際に不可欠です。

対象製品

このドキュメントは、下記の製品を対象としています。

・ チャートレコーダ	μR10000/μR20000
・ ペーパレスレコーダ	GX10/GX20/GP10/GP20、DX1000T/DX2000T、DX1000/DX2000/DX1000N、CX1000/CX2000
・ データアクイジションシステム	GM
・ データアクイジションユニット	MW100
・ シングルループコントローラ	YS1000シリーズ
・ ディジタル指示調節計/プログラム調節計/ディジタル指示警報計	UTAdvanced

商　　標

・Ethernetは、富士ゼロックス株式会社の登録商標です。
・Modbusは、米国 Schneider Automation Inc.の登録商標です。
・その他、本文中に使われている会社名・商品名は、各社の登録商標または商標です。
・本文中の各社の登録商標または商標には、TM、®マークは表示しておりません。

2. 保護すべき資産について

お客様資産を安心、安全に保つためには、まず、保護すべき資産をリストアップして、所有者を明確にし、それぞれの資産価値を評価する必要があります。資産価値が大きいほどセキュリティ対策の重要度が高くなります。保護すべき資産の例として次のようなものが挙げられます。

データ資産の例

- 生産スケジュール情報
- システム設定情報
- アプリケーション設定情報
- 制御パラメータ情報
- レシピ情報
- 履歴情報

デバイス資産の例

- エンジニアリングワークステーション（EWS）
- オペレータコンソール（OIT）
- プロセスコントローラ（DCS、PLC）
- フィールドデバイス
- ネットワークデバイス

人、環境資産の例

- 従業員
- 工場、プラント設備
- 自然環境

これらの資産が、セキュリティの脅威にさらされると、

- 生産活動の混乱や停止
- レシピなど、生産活動にかかわる機密情報の漏洩
- 人への損傷
- 工場／プラント設備の破壊
- 環境破壊

などを引き起こし企業に甚大な損失を与える可能性があります。

これらの資産を脅威から保護し、企業が受ける機会損失を低減させることが、セキュリティ対策の目的です。

重要度の分類例

下記に資産の重要度の分類例を示します。

- 重要度　A：極めて高い
- 重要度　B：高い
- 重要度　C：低い
- 重要度　D：極めて低い

補足
本　書　は、「ISA 99.00.01-2007: Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models」を参考にしています。本書では、この規格を ISA 99.00.01 と記述します。

「ISA 99.00.01」には、セキュリティ対策活動を決めるための "Activity-based criteria"（行動の判断基準）と、保護する資産を決めるための "Asset-based criteria"（資産の判断基準）が定義されています。本書は、これらの "criteria"（判断基準）を参考にしています。

3. 脅威の識別と評価ついて

リストアップされた保護すべき資産に対して、考えられるセキュリティ上の脅威を明確にします。脅威をリストアップするにあたっては、下記のような視点から考える必要があります。

悪意を持った人による資産への不正アクセス

- 社内の人
- 社外の人
- ネットワーク経由
- 資産への直接アクセス（資産が置かれている機器の直接操作）

悪意を持ったソフトウェアによる資産への不正アクセス

- ネットワーク経由
- リムーバブルメディア経由

正当な利用者の誤操作・不注意による偶発的な資産への不正アクセス

- ネットワーク経由
- リムーバブルメディア経由
- 資産への直接アクセス（資産が置かれている機器の直接操作）

識別されたセキュリティ上の脅威に対して、その発生可能性のレベルを評価します。発生可能性のレベルの分類例を下記に示します。

- 発生可能性レベルA：発生する可能性が高い
- 発生可能性レベルB：発生する可能性が中程度
- 発生可能性レベルC：発生する可能性は低い

脆弱性の識別と評価ついて

各資産に対する脆弱性、あるいは資産を格納した機器の脆弱性を明確にします。脆弱性とは、セキュリティ上の脅威が資産に悪影響を及ぼすことを許してしまう状態や条件のことをいいます。脆弱性としては下記のような例が挙げられます。

- セキュリティ対策の計画の不備
- セキュリティ対策の活動の不備
- セキュリティ対策の監督や改善の不備
- 物理的な保護の欠如
- 外部ネットワークへの接続点に置かれたファイアウォールの設定の不備
- ウィルスの駆除やセキュリティパッチの適用の不備
- バックアップの不備（システムのバックアップがされていない）
- 生産・制御システムやその操作・環境に対する理解不足
- システムの設計・操作に携わるスタッフのセキュリティ意識の欠如

リスクアセスメント

各資産あるいは、資産を格納している機器に対するセキュリティ上のリスクを評価します。リスクは次式で表現できるものと想定します。

リスク＝[脅威]×[脆弱性]×[想定される損害]

リスクアセスメントを実施することで、セキュリティ対策の優先順位を明確にすることができます。リスクアセスメントにおいては、たとえば、システムのある機能の停止による営業上の損失や、生産制御システムの損傷を修復するための費用を見積もります。

リスクの定量的な損害の度合いにより、個々のセキュリティ対策の実施について優先順位を決定します。その結果、どのリスクに対して対策をとらねばならないのか、どのリスクが許容範囲内かなど、具体的な対策を取る必要がある部分を明確にできます。

ただし、損害の中には、環境や人命に影響をおよぼすものや、企業の社会的信用なども含まれるため、一様な営業損失金額として見積もることが難しい場合があります。

4. 本ドキュメントの対象製品群の概要

対象製品

このドキュメントは、下記の製品を対象としています。

- チャートレコーダ　μR10000/μR20000
- ペーパレスレコーダ　GX10/GX20/GP10/GP20、DX1000T/DX2000T、DX1000/DX2000/DX1000N、CX1000/CX2000
- データアクイジションシステム　GM
- データアクイジション ユニット　MW100
- シングルループコントローラ　YS1000シリーズ
- ディジタル指示調節計/プログラム調節計/ディジタル指示警報計　UTAdvanced

対象製品はシリーズ毎に実装している通信機能が異なります。以下に、それぞれの製品シリーズごとに実装している通信機能、考慮すべきセキュリティ対策の要件を記載します。

対象製品の特徴

本書で紹介する全ての製品はマイクロプロセッサとリアルタイムOSを利用して通信アプリケーションを実行しています。通信アプリケーションは、製品シリーズごとに異なったものが工場で組み込まれます。

ユーザがこれらの機器に新しいプログラムコードを追加したり、新しいアプリケーションを生成したりすることは原則できません。例外的に製品に組み込むソフトウェアをユーザが自分で更新できるものもありますが、指定の方法による特定のコードの組み込みしか許されていないため、これによって悪意のあるプログラムが混入する怖れはありません。

通信プロトコル

EthernetとTCP/IPプロトコル

対象製品には10BASE-Tあるいは100BASE-TX Ethernetポートが標準あるいはオプションで装備されます。Ethernetを利用した通信には、安定したIPv4をベースにしたTCP、UDPプロトコルを使用しています。

対象製品にはIPアドレスの他、サブネットマスクとデフォルトゲートウェイを設定できます。
また、クライアント機能を搭載した対象製品では接続先のサーバー機器をIPアドレスで指定できる他、DNS (Domain Name System)を利用したホスト名での指定も可能です。

下表のポート番号は対象製品のサーバ機能への接続のために用意された工場出荷時の初期値のポート番号になります。ポート番号は、製品によっては固定である場合があります。表中に固定と記載されたポート番号は固定です。

ペーパレスレコーダGX10/GX20/GP10/GP20、データアクイジションシステムGM（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
502/tcp	4	Modbus	マルチ ベンダ接続（Modbus サーバ）
21/tcp	4	FTP または FTPS(暗号化 On 時)	ファイル転送（FTP サーバ）
44818/tcp	10	EtherNet/IP	マルチベンダ接続（EtherNet/IP サーバ）
44818/udp、2222/udp	-		
4840	3 セッション	OPC-UA	マルチベンダ接続（OPC-UA サーバ）
80/tcp または 443/tcp(暗号化 On 時)	-	HTTP または HTTPS(暗号化 On 時)	www（HTTP サーバ）
123/udp	-	SNTP	時刻同期（SNTP サーバ）
34434/tcp（固定）	4	横河独自	汎用通信サービス

データアクイジションユニットMW100（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
502/tcp	4	Modbus	マルチベンダ接続（Modbus サーバ）
21/tcp	4	FTP	ファイル転送（FTP サーバ）
80/tcp	-	HTTP	www（HTTP サーバ）
123/udp	-	SNTP	時刻同期（SNTP サーバ）
34318/tcp	4	横河独自	汎用通信サービス

ペーパレスレコーダDX1000T/DX2000T、DX1000/DX2000/DX1000N（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
502/tcp	2	Modbus	マルチベンダ接続（Modbus サーバ）
44818/tcp	10	EtherNet/IP	マルチベンダ接続（EtherNet/IP サーバ）
44818/udp、2222/udp	-		
21/tcp	2	FTP	ファイル転送（FTP サーバ）
80/tcp	-	HTTP	www（HTTP サーバ）
123/udp	-	SNTP	時刻同期（SNTP サーバ）
34260/tcp（固定）	3	横河独自	設定・測定サービス
34261/tcp（固定）	1	横河独自	保守・診断サービス
34264/udp（固定）	-	横河独自	機器情報サービス

ペーパレスレコーダCX1000/CX2000（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
21/tcp（固定）	2	FTP	ファイル転送（FTP サーバ）
80/tcp（固定）	-	HTTP	www（HTTP サーバ）
34260/tcp（固定）	3	横河独自	設定・測定サービス
34261/tcp（固定）	1	横河独自	保守・診断サービス
34264/udp（固定）	-	横河独自	機器情報サービス

チャートレコーダμR10000/μR20000（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
34260/tcp（固定）	3	横河独自	設定・測定サービス
34261/tcp（固定）	1	横河独自	保守・診断サービス
34264/udp（固定）	-	横河独自	機器情報サービス

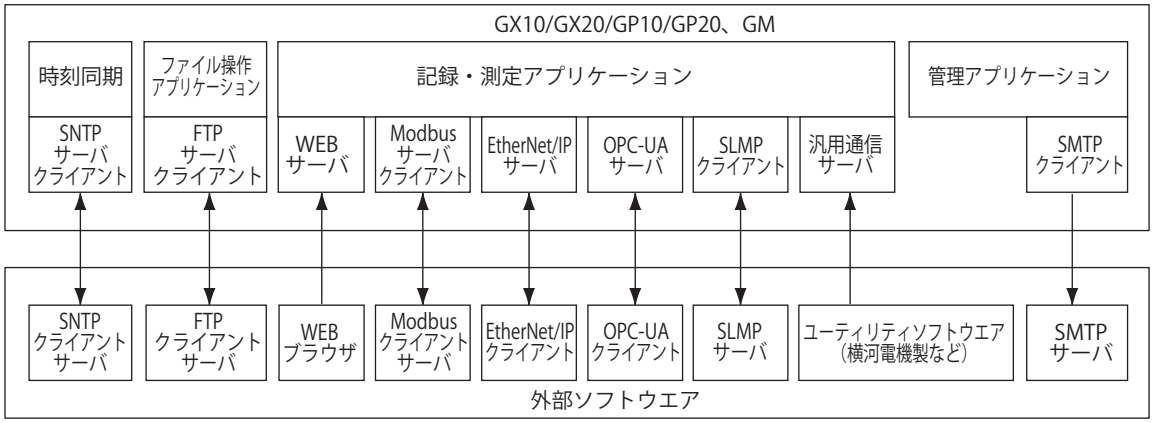
シングルループコントローラYS1000 シリーズ（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
502/tcp	2	Modbus	マルチベンダ接続（Modbus サーバ）

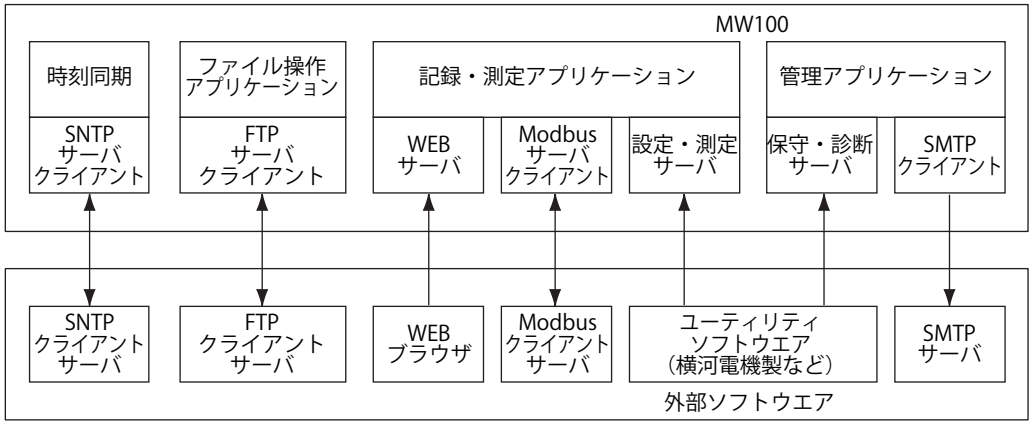
ディジタル指示調節計/プログラム調節計/ディジタル指示警報計UTAdvanced（サーバ機能一覧）

ポート番号	最大同時接続数	プロトコル	サービス
502/tcp	2	Modbus	マルチベンダ接続（Modbus サーバ）

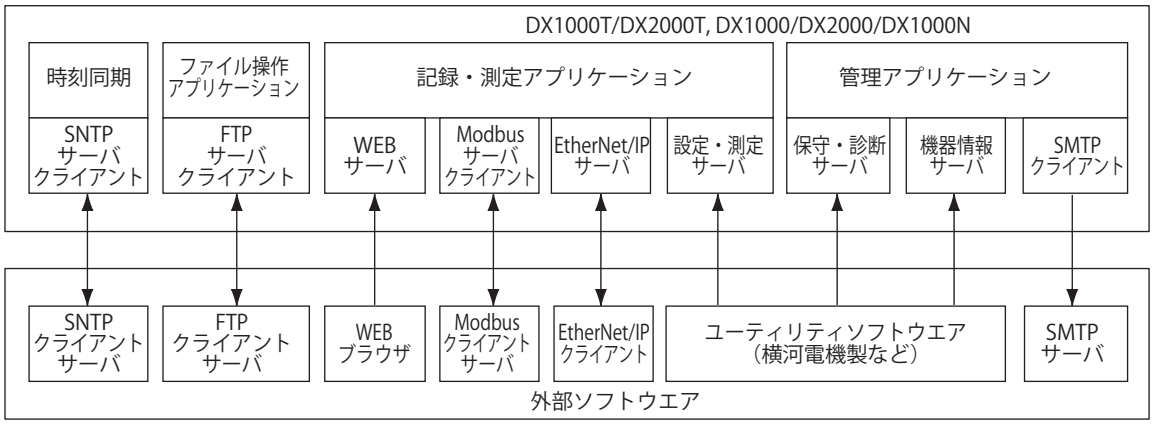
次の図は各機器のクライアントとサーバをまとめて示したものです。それぞれのプロトコルの概要を以下にまとめます。



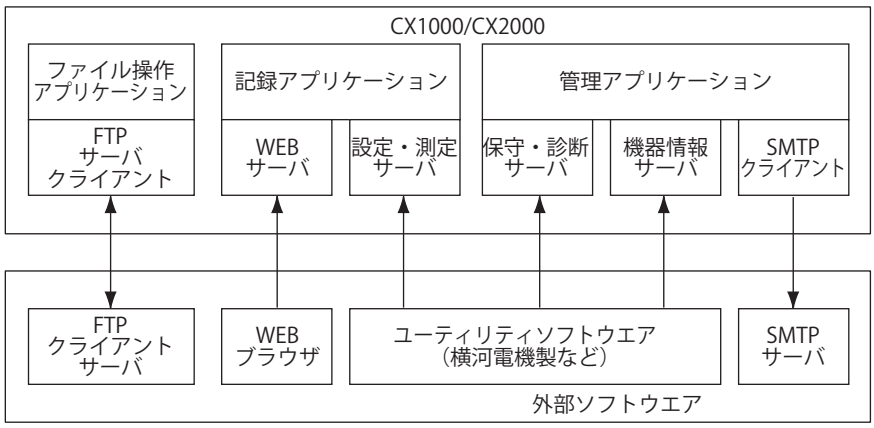
ペーパレスレコーダGX10/GX20/GP10/GP20、データアクイジションシステムGM



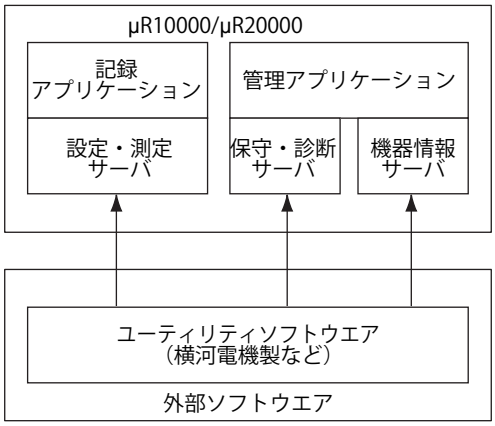
データアクイジションユニットMW100



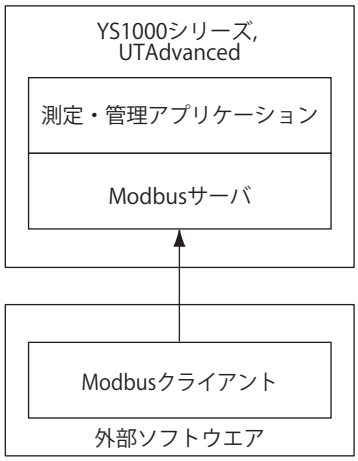
ペーパレスレコーダDX1000T/DX2000T、DX1000/DX2000/DX1000N



ペーパレスレコーダCX1000/CX2000



チャートレコーダμR10000/μR20000



シングルループコントローラYS1000シリーズ、ディジタル指示調節計/プログラム調節計/ディジタル指示警報計UTAdvanced

EtherNet/IPプロトコル(GX10/GX20/GP10/GP20、GM、DX1000T/DX2000T/DX1000/DX2000/DX1000Nで対応)

産業用の機器間通信で使われるプロトコルでPLC等と接続する際などに用いられます。GX10/GX20/GP10/GP20、GM、DX1000T/DX2000T/DX1000/DX2000/DX1000NではEtherNet/IPプロトコルを利用して測定データを入出力できます。

OPC-UAプロトコル(GX10/GX20/GP10/GP20、GMで対応)

産業用の機器間通信で使われるプロトコルで、SCADA、MES等と接続する際などに用いられます。GX10/GX20/GP10/GP20、GMではOPC-UAサーバ機能を利用してSCADA等の上位システム（OPC-UAクライアント）から測定データや設定情報を取得できます。

SLMPプロトコル(GX10/GX20/GP10/GP20、GMで対応)

産業用の機器間通信で使われるプロトコルで、主に三菱電機社製PLCと接続する際などに用いられます。GX10/GX20/GP10/GP20、GMではSLMPプロトコルを利用して測定データを入出力できます。

SNTPプロトコル(MW100、GX10/GX20/GP10/GP20、GM、DX1000T/DX2000T/DX1000/DX2000/DX1000Nで対応)

TCP/IPネットワークを通じて時刻を同期させるプロトコルです。MW100、GX10/GX20/GP10/GP20、GM、DX1000T/DX2000T/DX1000/DX2000/DX1000NではSNTPプロトコルを利用して、時刻情報の取得と提供ができます。

FTPプロトコル(ペーパレスレコーダ、GM、MW100で対応)

ファイル操作アプリケーションは、主記憶上に作成されたデータをファイルとして外部メディアに保存します。設定により、日報･週報などのレポートファイルを生成します。これらのファイルは、本体に内蔵された外部メディア（ディスクやメモリカード）上に保存されます。

FTPサーバを使って外部メディア上のファイルやディレクトリを操作できます。上記の測定値ファイルやレポートファイルは指定したディレクトリに保存されています。認証されたユーザはファイルを取り出したり、消去したり、新しいファイルを置いたりできます。FTPクライアントが活性化されていると、新しくファイルが作られたときなどに登録されたFTPサーバへファイルを転送できます。また、FTPサーバにはユーザ認証機能があり、後述するログイン機能を有効にするとユーザ、パスワードを入力しないと利用できなくすることができます。

接続先サーバは2台（プライマリとセカンダリ）まで登録でき、それぞれサーバ名（ホスト名またはIPアドレス）、ユーザ名とパスワード、初期ディレクトリを設定します。通常はプライマリサーバへの転送を試みますが、失敗した場合はセカンダリサーバへの転送を試みます。

HTTPプロトコル(ペーパレスレコーダ、GM、MW100で対応)

記録アプリケーションは遠隔のWebブラウザ上に記録画面やメッセージを表示したり、Webブラウザ経由で製品本体を遠隔操作したり（オペレータとしてログインした場合のみ）できるようにします。Webブラウザとしてはマイクロソフトのインターネット･エクスプローラでの動作が確認されています。また、HTTPサーバにはユーザ認証機能があり、後述するログイン機能を有効にするとユーザ、パスワードを入力しないと利用できなくすることができます。

SMTPプロトコル(ペーパレスレコーダ、GM、MW100で対応)

管理アプリケーションは、設定に従ってSMTPサーバに電子メールを発信することができます。対象製品で規定されているメール発信要因は以下の4つです：

（1）定周期
（2）ハードウエア故障などのシステムエラーの発生時
（3）時報・日報・月報などのレポートの作成時
（4）測定値の異常などによるアラームの発生時

それぞれの要因ごとにメール発信の有無、件名、宛先（2グループそれぞれへの送信の有無）、本文中の文章、オプションとして各機器のWebアドレス（URL）と測定値を付加するかを設定します。

Modbusプロトコル
(YS1000シリーズ、UTAdvanced、MW100、GM、GX10/GX20/GP10/GP20、DX1000T/DX2000T、DX1000/DX2000/DX1000Nで対応)

産業用の機器間通信で広く使われているプロトコルで、これらの機器をDCSやPLC、SCADA等と接続する際などに用いられます。GX10/GX20/GP10/GP20、GM、DX1000T/DX2000T/DX1000/DX2000/DX1000NではModbusプロトコルを利用して測定データを出力したり、測定のスタートストップ等を制御できます。YS1000シリーズ、UTAdvancedではModbusプロトコルでアクセスできるレジスタの値を変更することにより、機器のSP等の設定情報を外部より変更する事ができます。

横河独自プロトコル
(チャートレコーダ、ペーパレスレコーダ、データアクイジションユニットで対応)

記録アプリケーションと管理アプリケーションが 持っているサーバ機能は、コマンド/レスポンス型のプロトコルを使っています。測定値の読み出しや設定・測定、保守・診断情報や機器情報の読み出しが行えます。コマンド/レスポンスは基本的に文字列や数字からなるアスキー文字列でやり取りされますが、コマンドによってはバイナリ形式でレスポンスデータの通信が行われることがあります。コマンドとレスポンスの書式と動作は、個々の機器の取扱説明書に定義されています。また、横河独自プロトコルにはユーザ認証機能があり、後述するログイン機能を有効にするとユーザ、パスワードを入力しないと利用できなくすることができます。

5. セキュリティ上の危険性について

以下に留意すべきセキュリティ上の危険性を列記します。

マルウェア（ウイルス）感染の危険性

本ドキュメントの対象製品のオペレーティングシステム（OS）は組み込み用の特殊なものであり、多くのウイルスやマクロが標的としている市販のオフィスソフト、メールソフト、インターネット閲覧ソフトなどの組み込みもないので、マルウェア感染の可能性は非常に限定的です。しかし、DX、MW等の外部メディアを持つ機器はウィルスを含んだファイルの置き場（踏み台）として利用される危険性があるため、外部メディアの取り扱いには十分注意してください。

侵入の危険性

製品にログインすることで、複数のサーバ機能を利用することができます。
これらのサーバ機能、測定値、設定へ第三者から不正にアクセスされることがないよう、機器への直接のアクセスおよびネットワーク経由でのアクセスをパスワードで保護することができます。パスワードで保護するためには、ログイン機能を予めオンにしてください。HTTP、FTP経由のログインではユーザ名とパスワードが平文で転送されるため、ネットワークを盗聴されるとパスワードが漏洩する危険性があります。インターネットなど信頼できない場所からアクセスされる際は、HTTPSあるいはFTPSのような安全な通信をご利用ください。
もちろん、不注意な人による漏洩の危険は常にあります。各機器への直接侵入は遠隔サイトに設置して電話接続したりするときに発生する危険があり、予想される被害はデータの漏洩と設定の破壊、および出力系の不正操作による生産設備や製品の破損などさまざまです。

情報漏洩や破壊工作の危険性

チャートレコーダやシングルループコントローラ、ディジタル指示調節計ではネットワークに関する極めて限定された情報のみしか保持していません。（IPアドレス、サブネットマスク、デフォルトゲートウェイ、製品のホスト/ドメイン名およびDNSサーバのIPアドレス）

一方、ペーパレスレコーダ、データアクイジションユニットはFTPクライアント機能やSMTP機能を保有するため、外部のFTPサーバやSMTPサーバに関するアクセス情報を機器内に保有しています。ログインパスワードの漏洩や盗聴により機器への不正侵入が行われ、これらのアクセス情報が漏れた場合には、当該サーバへの不正侵入につながるかもしれません。

機器への不正侵入ではこの他に、測定値を取り出されたり、設定を破壊されたり、出力（制御信号）を不正に操作される危険もあります。たとえば、設定値を外部から故意に変更される事で制御している温度が異常に上げられると生産品が被害を受けるかもしれません。また、記録データを消去されたり、別のデータで改ざんされる可能性もあります。

このような情報漏洩や破壊工作は、機器への不正侵入をもとに行われることが多いため、侵入への対策として記載したログイン機能、HTTPSやFTPSによる安全な通信などの利用が対策として有効です。

6. 製品固有のセキュリティ機能

ここでは、セキュリティ対策を施す際に考慮すべき各システム製品のセキュリティ機能について説明します。各製品には、セキュリティ強化のための機能が用意されています。

ペーパレスレコーダGX10/GX20/GP10/GP20、データアクイジションシステムGM

ログイン機能

本製品群へのアクセスを、あらかじめ登録されたユーザだけに制限する機能です。
ログイン機能をONにし、管理者権限、利用者権限を設定する事で、機器にアクセスし測定データを閲覧する人、機器にアクセスし測定設定情報を変更する人を限定できます。
これにより、ネットワーク越しあるいは直接端末にアクセスされた場合、さらには物理的に端末を盗難された場合も、権限のない第三者が不正な操作・設定を行うことができず、測定値や設定など重要データの盗難・改ざん・削除を防ぐことができます。
登録ユーザレベル（権限）には次の２種類があります。

管理者権限	全ての機能を利用できます。 どの機能を一般ユーザに開放するか、操作・設定権限をユーザごとに設定できます。
一般ユーザ権限	FTPでの外部メディアの書き込み等に制限があります。 測定データ、レポートデータ、ログ情報、ステータス情報等を取得できます。操作・設定権限は個別に設定できます。

セキュリティ確保のため、個別ユーザに必要な最小限の権限を割り当てて使用してください。これらの機器では最大50名の管理者と一般ユーザを登録可能です。

SSL通信機能

遠隔地からのアクセスでは、情報を暗号化して送受信するプロトコル、SSL (Secure Socket Layer)を使った通信が可能です。公開鍵暗号と証明書を利用し、通信の暗号化、接続先の認証を行います。これにより、認証された正規の端末／ユーザからのアクセスだけを許可し、第三者からの不正アクセスによる重要データの盗難・改ざん・削除を防ぐことができます。HTTPサーバとFTPサーバの通信を暗号化するHTTPS、FTPS通信に対応しています。

IPアクセス制限機能

登録されたIPアドレスからのModbusアクセスのみ許可し、未登録のIPアドレスからのアクセスを拒否します。この機能を利用する事で、Modbus経由の不正アクセスを防止し、重要データの盗難・改ざん・削除を防ぐことができます。

ログ情報

通信ログや操作ログ、FTP等のログを参照することで機器に対して行われた操作を把握することができます。これにより、万が一、機器に対して不正な操作・設定が行われた場合に、ログを解析することで、原因を分析し、適切な対処を行うことができます。

サイバー攻撃に対する堅牢性

GM10、GX10、GX20、GP10およびGP20は、産業用機器の堅牢性を認証するAchillesレベル1認証相当の通信テストにおいて、記録機能が健全に動作することを確認済みです。

- 上記内容は、以下のRev以降で確認済みです。
  GM10：R4.01.01
  GX10：R4.01.01
  GX20：R4.01.01
  GP10：R4.01.01
  GP20：R4.01.01

- Achilles認証の詳細は、以下をご参照ください。
  http://www.wurldtech.com/certifications/achilles-communications-certification

データアクイジションユニットMW100

ログイン機能

MW100と通信する際に、あらかじめ登録されたユーザだけアクセスできる機能です。ユーザレベル（権限）には次の２種類があります。

管理者権限	全ての機能を利用できます。
利用者権限	FTPでの外部メディアの書き込み等に制限があります。 測定データ、レポートデータ、ログ情報、ステータス情報等を取得できます。測定レンジの変更等には、管理者権限が必要です。

ログイン機能をONにし、管理者権限、利用者権限を設定する事でMW100にアクセスし測定データを閲覧する人、MW100にアクセスし測定設定情報を変更する人を限定できます。セキュリティ確保のため、ユーザの権限にあわせて割り当てて使用してください。MW100では最大10名まで登録可能です。

ログ情報

通信ログや操作ログ、FTP等のログを参照することで機器に対して行われた操作を把握することができます

ペーパレスレコーダDX1000T/DX2000T、DX1000/DX2000/DX1000N

ログイン機能

上記ペーパレスレコーダと通信する際に、あらかじめ登録されたユーザだけアクセスできる機能です。ユーザレベル（権限）には次の２種類があります。

管理者権限	全ての機能を利用できます。 どの機能を一般ユーザに開放するか設定できます。
一般ユーザ権限	FTPでの外部メディアの書き込み等に制限があります。 測定データ、レポートデータ、ログ情報、ステータス情報等を取得できます。測定レンジの変更等には管理者権限が必要です

ログイン機能をONにし、管理者権限、利用者権限を設定する事でペーパレスレコーダにアクセスし測定データを閲覧する人、ペーパレスレコーダにアクセスし測定設定情報を変更する人を限定できます。セキュリティ確保のため、ユーザの権限にあわせて割り当てて使用してください。これらのペーパレスレコーダでは最大で管理者5名と30名までの一般ユーザを登録可能です。

アクセス制限機能 (DX1000T/DX2000T、DX1000/DX2000/DX1000N Release 3以降に搭載、Modbusサーバ限定)

登録されたIPアドレスからのModbusアクセスのみ許可し、未登録のIPアドレスからのアクセスを拒否します。この機能を利用する事で、Modbus経由の不正アクセスを防止し、重要データの盗難・改ざん・削除を防ぐことができます。

ログ情報

通信ログや操作ログ、FTP等のログを参照することで機器に対して行われた操作を把握することができます。これにより、万が一、機器に対して不正な操作・設定が行われた場合に、ログを解析することで、原因を分析し、適切な対処を行うことができます。

ペーパレスレコーダCX1000/CX2000

ログイン機能

上記ペーパレスレコーダと通信する際に、あらかじめ登録されたユーザだけアクセスできる機能です。ユーザレベル（権限）には次の２種類があります。

管理者権限	全ての機能を利用できます。
利用者権限	FTPでの外部メディアの書き込み等に制限があります。 測定データ、レポートデータ、ログ情報、ステータス情報等を取得できます。測定レンジの変更等には、管理者権限が必要です。

ログイン機能をONにし、管理者権限、利用者権限を設定する事でペーパレスレコーダにアクセスし測定データを閲覧する人、ペーパレスレコーダにアクセスし測定設定情報を変更する人を限定できます。セキュリティ確保のため、ユーザの権限にあわせて割り当てて使用してください。これらのペーパレスレコーダでは管理者1名と最大6名までの利用者を登録可能です。

ログ情報

通信ログや操作ログ、FTP等のログを参照することで機器に対して行われた作業を把握することができます。

ディジタル指示調節計/プログラム調節計/ディジタル指示警報計UTAdvanced

Modbusレジスタへの書き込み許可の設定

通信によるModbusレジスタへの書き込みを許可または禁止することができます。通信による書き込みを禁止すれば外部から悪意を持ったものが、調節計の設定を変更する事を防げます。この場合、設定変更は現場にて手動で行う必要があります。

IPアクセス制限機能

登録されたIPアドレスからのModbusアクセスのみ許可し、未登録のIPアドレスからのアクセスを拒否します。この機能を利用する事で、不正アクセスを防止し、セキュリティを高めることができます。

シングルループコントローラYS1000シリーズ

Ethernetからの書き込み可否の設定

Ethernet通信によるModbusレジスタへの書き込みを許可または禁止することができます。通信による書き込みを禁止すれば外部から悪意を持ったものが、コントローラの設定を変更する事を防げます。この場合、設定変更は現場にて手動で行う必要があります。

サイバー攻撃に対する堅牢性

YS1000は、産業用機器の堅牢性を認証するAchillesレベル1認証相当の通信テストにおいて、制御機能が健全に動作することを確認済みです。

- 上記内容は、以下のRev以降で確認済みです。
  YS1000：MCU R2.01.01、DCU R2.01.02、NCU R2.01.02
- Achilles認証の詳細は、以下をご参照ください。
  http://www.wurldtech.com/certifications/achilles-communications-certification

7. スタッフのセキュリティ

セキュリティ問題につながる可能性のある重要な脅威の一つが“人”です。人による誤操作などが脅威となります。

教育

教育の目的は、スタッフが、セキュリティの知識と技能を持ち、日常の業務の中でセキュリティ対策の規範に従った行動を取れるようにすることです。教育が含むべき項目を示します。

- スタッフのセキュリティに対する理解を深める。
- スタッフが、生産制御システムに対する脅威と影響を正しく認識する。
- スタッフが、セキュリティ対策や改善を適切に行えるようにする。
- スタッフが、生産・制御システムに対する正しい操作と管理の仕方を理解する。
  たとえば、システムに対する攻撃の有無を確認できるようなログの確認方法を理解する。

教育は、下記のようなタイミングで実施すべきです。

- 採用時
- 人事異動などによりアクセスする対象が変わった時

技術資料　改訂情報

資料名称　　：レコーダ＆データロガー / 小規模計装機器向けセキュリティ対策基準

資料番号　　：TI 04A02A01-00JA

2009年9月／初版
新規発行

2012年11月／2版
SMARTDAC+ GX/GP 追加

2015年8月／3版
SMARTDAC+ GM 追加

2016年11月／4版
プロトコル説明の追加

2017年7月／5版
内容の見直し